AZ EURÓPAI UNIÓ ÉS A SVÁJCI ÁLLAMSZÖVETSÉG KÖZÖTTI, AZ UNIÓS ÉS A SVÁJCI KIBOCSÁTÁSKERESKEDELMI RENDSZER ÖSSZEKAPCSOLÁSÁRÓL SZÓLÓ MEGÁLLAPODÁSSAL LÉTREHOZOTT VEGYES BIZOTTSÁG 2/2020. számú határozata

(2020. november 5.)

a megállapodás I. és II. mellékletének módosításáról, valamint kapcsolástechnikai szabványok (Linking Technical Standards – LTS) elfogadásáról [2021/1034]

A VEGYES BIZOTTSÁG,

tekintettel az Európai Unió és a Svájci Államszövetség közötti, az uniós és a svájci kibocsátáskereskedelmi rendszer összekapcsolásáról szóló megállapodásra ([1]) (a továbbiakban: a megállapodás) és különösen annak 3. cikke (7) bekezdésére és 13. cikke (2) bekezdésére,

mivel:

(1) A vegyes bizottság 2019. december 5-i 2/2019. számú határozata ([2]) módosította a megállapodás I. és II. mellékletét, teljesítve ezáltal a megállapodásban az összekapcsolásra vonatkozóan meghatározott feltételeket.

(2) A vegyes bizottság 2/2019. számú határozatának elfogadását követően, a megállapodás 21. cikkének (3) bekezdése alapján a Felek kicserélték megerősítő, illetve jóváhagyó okirataikat, mivel az összekapcsolásnak a megállapodásban meghatározott valamennyi feltételét teljesítettnek tekintik.

(3) A megállapodás 21. cikkének (4) bekezdése értelmében a megállapodás 2020. január 1-jén hatályba lépett.

(4) A megállapodás I. mellékletét a megállapodás 13. cikke (2) bekezdésének megfelelően módosítani kell, figyelembe véve a kibocsátásiegység-forgalmi jegyzékek összekapcsolása terén elért eredményeket, annak érdekében, hogy az első alkalommal Svájchoz besorolt légijármű-üzembentartókkal kapcsolatos igazgatási feladatok tekintetében zökkenőmentes legyen az átmenet.

(5) A közelmúlt fejleményeihez való igazodás, valamint a kibocsátásiegység-forgalmi jegyzékek összekapcsolása tekintetében a megállapodás által megkövetelt rugalmasság növelése érdekében módosítani kell a megállapodás II. mellékletét a megállapodás 13. cikkének (2) bekezdésével összhangban, a kibocsátásiegység-forgalmi jegyzékek közötti kapcsolat létrehozásához szükséges nagyobb, de egyenértékű technológiai eszköztár elérhetővé tétele érdekében.

(6) A megállapodás 3. cikkének (7) bekezdése értelmében a svájci jegyzékkezelőnek és az uniós központi tisztviselőnek ki kell dolgoznia a kapcsolástechnikai szabványokat (Linking Technical Standards – LTS), amelyek a II. mellékletben foglalt elveken alapulnak. Az LTS-eknek ismertetniük kell a svájci kiegészítő ügyleti jegyzőkönyv (SSTL) és az európai uniós ügyleti jegyzőkönyv (EUTL) közötti stabil és biztonságos kapcsolat létrehozásának részletes követelményeit. Az LTS-ek a vegyes bizottság határozatával történő elfogadásukat követően lépnek hatályba.

(7) A megállapodás 13. cikkének (1) bekezdése szerint a vegyes bizottság technikai iránymutatásokat fogad el a megállapodás megfelelő végrehajtásának biztosítása érdekében, ideértve az SSTL és az EUTL közötti stabil és biztonságos kapcsolat létrehozását. A megállapodás 12. cikkének (5) bekezdése szerint felállított munkacsoport dolgozhat ki technikai iránymutatásokat. A munkacsoportban részt kell vennie legalább a svájci jegyzékkezelőnek és az uniós központi tisztviselőnek, és a munkacsoportnak segítenie kell a vegyes bizottságot a megállapodás 13. cikke szerinti feladatai elvégzése során.

(8) Tekintettel az iránymutatások műszaki jellegére, valamint arra, hogy azokat hozzá kell igazítani a műszaki fejlődéshez, a svájci jegyzékkezelő és az uniós központi tisztviselő által kidolgozott technikai iránymutatásokat tájékoztatás céljából, illetve – adott esetben – jóváhagyás céljából be kell nyújtani a vegyes bizottságnak,

([1]) HL L 322., 2017.12.7., 3. o.

([2]) Az Európai Unió és a Svájci Államszövetség közötti, az uniós és a svájci kibocsátáskereskedelmi rendszer összekapcsolásáról szóló megállapodás által létrehozott vegyes bizottság 2/2019. sz. határozata (2019. december 5.) az Európai Unió és a Svájci Államszövetség közötti, az uniós és a svájci kibocsátáskereskedelmi rendszer összekapcsolásáról szóló megállapodás I. és II. mellékletének módosításáról (HL L 314., 2020.9.29., 68. o.).

ELFOGADTA EZT A HATÁROZATOT:

1. cikk

A megállapodás I. melléklete B. részének 17. pontjában a második bekezdés helyébe a következő szöveg lép:

„Az e megállapodás hatálybalépését követően első alkalommal Svájchoz besorolt légijármű-üzembentartókkal kapcsolatos igazgatási feladatokat Svájc a besorolás évében április 30. után és a kibocsátásiegység-forgalmi jegyzékek közötti ideiglenes kapcsolat működőképessé válását követően látja el.”

2. cikk

A megállapodás II. mellékletének negyedik albekezdése helyébe a következő szöveg lép:

„Az LTS-ek előírják, hogy az SSTL és az EUTL közötti kommunikáció a webszolgáltatási üzeneteknek a következő technológiákon (*), illetve ezekkel egyenértékű technológiákon alapuló biztonságos cseréjéből áll:

– egyszerű objektumelérési protokollt (SOAP) használó webszolgáltatások,
– hardveralapú virtuális magánhálózat (VPN),
– XML (bővíthető jelölőnyelv),
– digitális aláírás, valamint
– hálózati idő protokollok (Network Time Protocol).

(*) E technológiákat jelenleg az uniós kibocsátásiegység-forgalmi jegyzék és a nemzetközi ügyleti jegyzőkönyv, valamint a svájci kibocsátásiegység-forgalmi jegyzék és a nemzetközi ügyleti jegyzőkönyv közötti kapcsolat létrehozására használják.”

3. cikk

Az e határozat mellékletét képező kapcsolástechnikai szabványok (LTS-ek) elfogadásra kerülnek.

4. cikk

A megállapodás 12. cikkének (5) bekezdése alapján egy munkacsoport jön létre. A munkacsoport segíti a vegyes bizottságot a megállapodás megfelelő végrehajtásának biztosításában, így többek között az LTS-ek végrehajtására irányuló technikai iránymutatások kidolgozásában.

A munkacsoportban részt vesz legalább a svájci jegyzékkezelő és az uniós központi tisztviselő.

5. cikk

Ez a határozat az elfogadásának napján lép hatályba.

Kelt Brüsszelben, 2020. november 5-én.

a vegyes bizottság részéről	az elnök	titkár Svájc részéről
titkár az Európai Unió részéről	Beatriz YORDI	Caroline BAUMANN
Maja-Alexandra DITTEL		

MELLÉKLET

Kapcsolástechnikai szabványok (LTS-ek) az Európai Unió és a Svájci Államszövetség közötti, az uniós és a svájci kibocsátáskereskedelmi rendszer összekapcsolásáról szóló megállapodás 3. cikkének (7) bekezdése alapján

IDEIGLENES MEGOLDÁSRA VONATKOZÓ ELŐÍRÁSOK

1. **Glosszárium**

1-1. táblázat

Üzleti rövidítések és fogalommeghatározások

Rövidítés/Kifejezés	Fogalommeghatározás
Kibocsátási egység	Egy meghatározott időszakban egy szén-dioxid tonna-egyenérték kibocsátására való jogosultság, amely csak az EU ETS vagy a svájci ETS szerinti követelmények teljesítésére érvényes.
CH	Svájci Államszövetség
CHU	Svájci általános célú kibocsátási egységek (a „CHU2” kifejezés használatos a 2. kötelezettségvállalási időszakra kiadott kibocsátási egységekre)
CHUA	Svájci légi közlekedési kibocsátási egység
COP	Közös üzemeltetési eljárások (Common Operational Procedures), melyeket a megállapodást aláíró Felek közösen dolgoztak ki az EU ETS és a svájci ETS összekapcsolásának működőképessé tétele érdekében.
ETR	Kibocsátásiegység-forgalmi jegyzék
ETS	Kibocsátáskereskedelmi rendszer
EU	Európai Unió
EUA	EU általános célú kibocsátási egység
EUAA	EU légi közlekedési kibocsátási egység
EUCR	Európai uniós konszolidált kibocsátásiegység-forgalmi jegyzék
EUTL	Európai uniós ügyleti jegyzőkönyv
Kibocsátásiegység-forgalmi jegyzék	Az ETS keretében kiadott kibocsátási egységek elszámolására szolgáló rendszer, amely nyomon követi az elektronikus számlákon tartott kibocsátási egységek tulajdonosait.
SSTL	Svájci kiegészítő ügyleti jegyzőkönyv
Ügylet	Olyan folyamat a kibocsátásiegység-forgalmi jegyzékben, amelynek keretében kibocsátási egységet vezetnek át egy számláról egy másikra.
Ügyleti jegyzőkönyv rendszer	Az ügyleti jegyzőkönyv feljegyzést tartalmaz az egyik kibocsátásiegység-forgalmi jegyzékből a másikba küldött minden egyes javasolt ügyletről.

1-2. táblázat

Műszaki rövidítések és fogalommeghatározások

Rövidítés	Fogalommeghatározás
Nyilvános kulcsú kriptográfia	Nyilvános és magánkulcsokat használ adatok titkosításához és visszafejtéséhez.
Tanúsító hatóság	Elektronikus tanúsítványokat kiállító szervezet.

Rövidítés	Fogalommeghatározás
Rejtjelezési kulcs	A rejtjelezési algoritmus funkcionális kimenetét meghatározó információ.
Visszafejtés	A titkosítással ellentétes folyamat.
Digitális aláírás	Üzenet, szoftver vagy elektronikus dokumentum eredetiségének és sértetlenségének a hitelesítésére alkalmazott matematikai módszer.
Titkosítás	Információk vagy adatok kóddá történő átalakítása, különösen jogosulatlan hozzáférés megakadályozása érdekében.
Fájl beolvasása	A fájl olvasásának folyamata.
Tűzfal	Hálózatbiztonsági készülék vagy szoftver, amely felügyeli és szabályozza a bejövő és kimenő hálózati forgalmat előre meghatározott szabályok alapján.
Szívdobbanás-felügyelet	Hardware vagy szoftver által létrehozott vagy felügyelt időszakos jel az üzemszerű működés jelzése vagy a számítógépes rendszer egyéb részeinek szinkronizálása érdekében.
IPSec	IP biztonság. Hálózati protokollkészlet, amely hitelesíti és titkosítja az adatcsomagokat két számítógép között IP-hálózaton keresztül történő biztonságos, titkosított kommunikáció biztosítása érdekében.
Behatolási tesztelés	Számítógépes rendszer, hálózat vagy webes alkalmazás támadók által kihasználható biztonsági sebezhetőségeinek felderítésére irányuló tesztelés.
Egyeztetési folyamat	Folyamat, amely biztosítja az egyezést két külön nyilvántartás között.
VPN	Virtuális magánhálózat.
XML	Bővíthető jelölőnyelv. Lehetővé teszi a tervezők számára saját, személyre szabott címkék létrehozását, lehetővé téve adatok meghatározását, továbbítását, hitelesítését és értelmezését alkalmazások között, valamint szervezetek között.

2. **Bevezetés**

Az Európai Unió és a Svájci Államszövetség közötti 2017. november 23-i, az uniós és a svájci kibocsátáskereskedelmi rendszer összekapcsolásáról szóló megállapodás (a továbbiakban: a megállapodás) rendelkezik az uniós kibocsátáskereskedelmi rendszerben (a továbbiakban: EU ETS) vagy a svájci kibocsátáskereskedelmi rendszerben (a továbbiakban: svájci ETS) felhasználható kibocsátási egységek kölcsönös elismeréséről. Az EU ETS és a svájci ETS összekapcsolásának működőképessé tétele érdekében az uniós kibocsátásiegység-forgalmi jegyzék európai uniós ügyleti jegyzőkönyve (EUTL) és a svájci kibocsátásiegység-forgalmi jegyzék svájci kiegészítő ügyleti jegyzőkönyve (SSTL) közötti közvetlen kapcsolatot hoznak létre, amely lehetővé teszi a két ETS bármelyikében kiadott kibocsátásiegység-forgalmi jegyzékek egymás közötti átruházását (a megállapodás 3. cikkének (2) bekezdése). Az EU ETS és a svájci ETS összekapcsolásának működőképessé tétele érdekében átmeneti megoldást kell bevezetni 2020 májusáig vagy azt követően a lehető leghamarabb. A Felek együttműködnek annak érdekében, hogy az ideiglenes megoldást a lehető leghamarabb kibocsátásiegység-forgalmi jegyzékek közötti állandó kapcsolatra cseréljék (a megállapodás II. melléklete).

A megállapodás 3. cikkének (7) bekezdése értelmében a svájci jegyzékkezelő és az uniós központi tisztviselő a megállapodás II. mellékletében foglalt elveken alapuló kapcsolástechnikai szabványokat (LTS-ek) dolgoz ki, amelyek tartalmazzák az SSTL és az EUTL közötti stabil és biztonságos kapcsolat létrehozásának részletes követelményeit. A jegyzékkezelő és a központi tisztviselő által kidolgozott LTS-ek azt követően lépnek hatályba, amikor a vegyes bizottság a határozatával elfogadja azokat.

Az ebben a dokumentumban rögzítettek szerint az LTS-eket a vegyes bizottság a 2/2020. számú határozatával fogadja el. E határozat értelmében a vegyes bizottság felkéri a svájci jegyzékkezelőt és az uniós központi tisztviselőt arra, hogy dolgozzanak ki további technikai iránymutatásokat az összekapcsolás működőképessé tétele érdekében, valamint azért, hogy biztosítsák azoknak a műszaki fejlődéshez, valamint a kapcsolat védelmére és biztonságára, illetve hatékony és eredményes működésére vonatkozó új követelményekhez való folyamatos hozzáigazítását.

2.1. *Alkalmazási kör*

Ez a dokumentum a megállapodás feleinek közös álláspontját képviseli az EU ETS és a svájci ETS kibocsátásiegység-forgalmi jegyzékei összekapcsolása műszaki alapjainak megteremtése tekintetében. Miközben felvázolja a műszaki előírások kiindulási alapját az architektúrára, a szolgáltatásra és a biztonságra vonatkozó követelményekkel összefüggésben, szükség lesz további részletes iránymutatásokra is a kapcsolat működőképessé tétele érdekében.

Megfelelő működéséhez a kapcsolat folyamatokat és eljárásokat igényel az összekapcsolás további működőképessége érdekében. A megállapodás 3. cikkének (6) bekezdése szerint ezeket a kérdéseket a közös üzemeltetési eljárásokat tartalmazó külön dokumentum részletezi, amelyet külön kell elfogadni a vegyes bizottság határozatával.

2.2. *Címzettek*

E dokumentum címzettje a svájci jegyzékkezelő és az uniós központi tisztviselő.

3. **Általános rendelkezések**

3.1. *A kommunikációs kapcsolat architektúrája*

E szakasz célja, hogy ismertesse az EU ETS és a svájci ETS közötti kapcsolat és annak különböző alkotóelemei működőképessé tételének általános architektúráját.

Mivel a biztonság a kibocsátásiegység-forgalmi jegyzékek közötti kapcsolat architektúrája meghatározásának kulcsfontosságú eleme, minden intézkedés megtételére sor került a stabil architektúra biztosítása érdekében. Bár a kibocsátásiegység-forgalmi jegyzékek között tervezett állandó kapcsolat webszolgáltatásokon fog alapulni, az ideiglenes kapcsolat fájlcserélő mechanizmust alkalmaz.

A műszaki megoldás az alábbiakat alkalmazza:

– biztonságos üzenettovábbítási protokoll,

– XML-üzenetek,

– XML-alapú digitális aláírás és titkosítás,

– VPN készülék vagy azzal egyenértékű biztonságos adatátviteli hálózat.

3.1.1. Üzenetváltás

Az uniós kibocsátásiegység-forgalmi jegyzék és a svájci kibocsátásiegység-forgalmi jegyzék közötti kommunikáció üzenetváltási mechanizmuson fog alapulni, biztonságos csatornákon keresztül. Mindkét oldal saját adattárral rendelkezik a beérkező üzenetek számára.

Mindkét Fél nyilvántartást vezet a beérkező üzenetekről és a feldolgozási adatokról.

A hibákat és a váratlan állapotokat figyelmeztetés formájában jelenteni kell, és szükség van a támogató csoportok közötti emberi kapcsolatra.

A hibák és a váratlan események kezelése során be kell tartani a közös üzemeltetési eljárásokban foglalt eseménykezelési folyamatban meghatározott üzemeltetési eljárásokat.

3.1.2. XML üzenet – Magas szintű leírás

Az XML üzenet az alábbiak egyikét tartalmazza:

– egy vagy több ügyleti kérelem és/vagy egy vagy több ügyleti válaszadás,

– egy művelet/válasz az egyeztetéshez kapcsolódóan,

– egy próbaüzenet.

Minden üzenet a következőket tartalmazó fejléccel rendelkezik:

– származási ETS rendszer,

– sorszám.

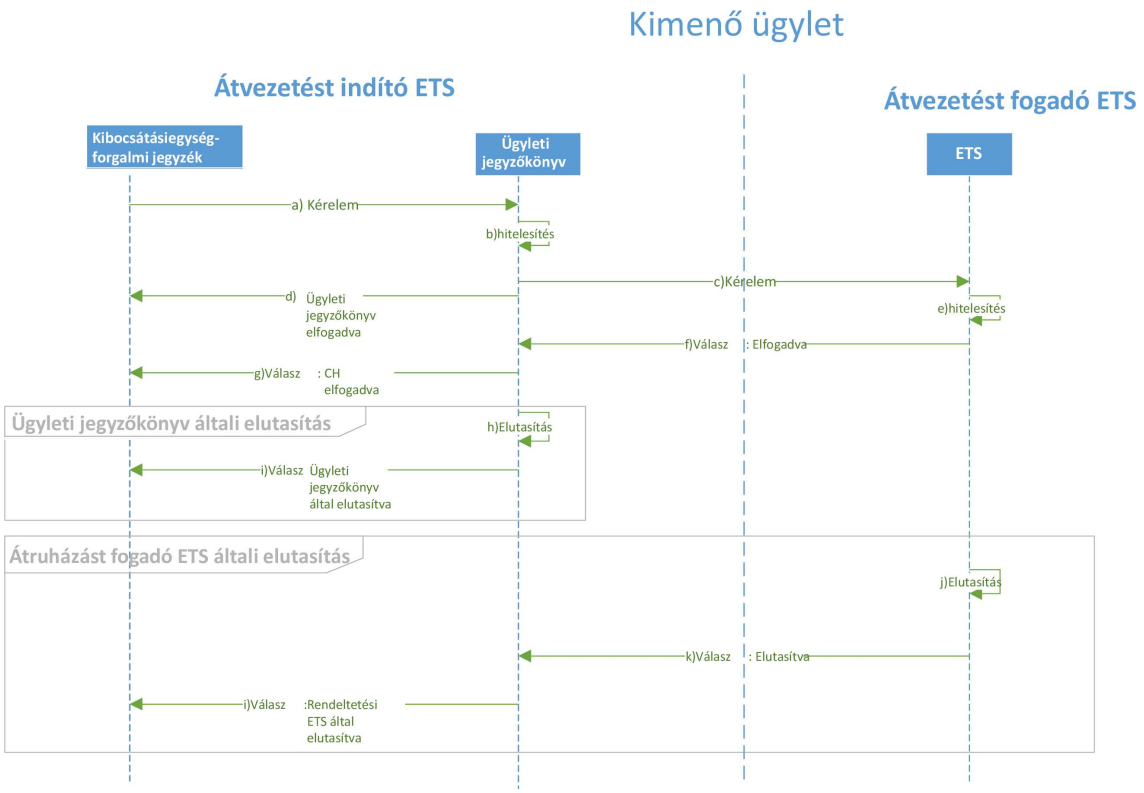
3.1.3. Befogadási ablakok

Az ideiglenes megoldás előre meghatározott befogadási ablakokon alapul, amelyeket megnevezett események csoportja követ. A kapcsolaton keresztül beérkező ügyleti kérelmek csak előre meghatározott időközönként kerülnek befogadásra. A befogadási ablakok magukban foglalják a kimenő és a bejövő ügyletek műszaki érvényesítését. Ezenfelül napi szintű egyeztetésekre kerülhet sor, amelyek manuálisan kezdeményezhetők.

Az ezen események bármelyikének a gyakoriságában és/vagy időzítésében bekövetkező változások kezelése során be kell tartani a közös üzemeltetési eljárásokban foglalt kérésteljesítési folyamatban meghatározott üzemeltetési eljárásokat.

3.1.4. Ügyleti üzenetek folyamata

Kimenő ügyletek



Ez az átvezetést indító ETS nézőpontját tükrözi. A fenti folyamatábra mutatja az összes konkrét folyamatot a kimenő ügyletek vonatkozásában.

Fő folyamat: „Szokásos ügylet” (a folyamat lépéseit a fenti rajz ábrázolja):

a) az átvezetést indító ETS-ben az ügyleti kérelmet elküldik a kibocsátásiegység-forgalmi jegyzékből az ügyleti jegyzőkönyvbe, amint valamennyi üzleti késedelem megszűnik (adott esetben 24 órás késedelem);

b) az ügyleti jegyzőkönyv érvényesíti az ügyleti kérelmet;

c) az ügyleti kérelmet elküldik a rendeltetési ETS-nek;

d) az elfogadó választ elküldik a származási ETS kibocsátásiegység-forgalmi jegyzékének;

e) a rendeltetési ETS érvényesíti az ügyleti kérelmet;

f) a rendeltetési ETS visszaküldi az elfogadó választ a származási ETS ügyleti jegyzőkönyvéhez;

g) az ügyleti jegyzőkönyv elküldi az elfogadó választ a kibocsátásiegység-forgalmi jegyzéknek.

Alternatív folyamat: „Ügyleti jegyzőkönyv általi elutasítás” (a folyamat lépéseit a fenti rajz ábrázolja, ebben az esetben is az a) ponttól kiindulva):

a) A származási ETS-ben az ügyleti kérelmet elküldik a kibocsátásiegység-forgalmi jegyzékből az ügyleti jegyzőkönyvbe, amint valamennyi üzleti késedelem megszűnik (adott esetben 24 órás késedelem).

Ezt követően:

b) az ügyleti jegyzőkönyv nem érvényesíti a kérelmet;

c) elutasító üzenetet küldenek a származási kibocsátásiegység-forgalmi jegyzékhez.

Alternatív folyamat: „ETS általi elutasítás” (a folyamat lépéseit a fenti rajz ábrázolja, az a) ponttól kiindulva):

a) a származási ETS-ben az ügyleti kérelmet elküldik a kibocsátásiegység-forgalmi jegyzékből az ügyleti jegyzőkönyvbe, amint valamennyi üzleti késedelem megszűnik (adott esetben 24 órás késedelem);

b) az ügyleti jegyzőkönyv érvényesíti az ügyletet;

c) az ügyleti kérelmet elküldik a rendeltetési ETS-nek;

d) az elfogadó üzenetet elküldik a származási ETS kibocsátásiegység-forgalmi jegyzékének.

Ezt követően:

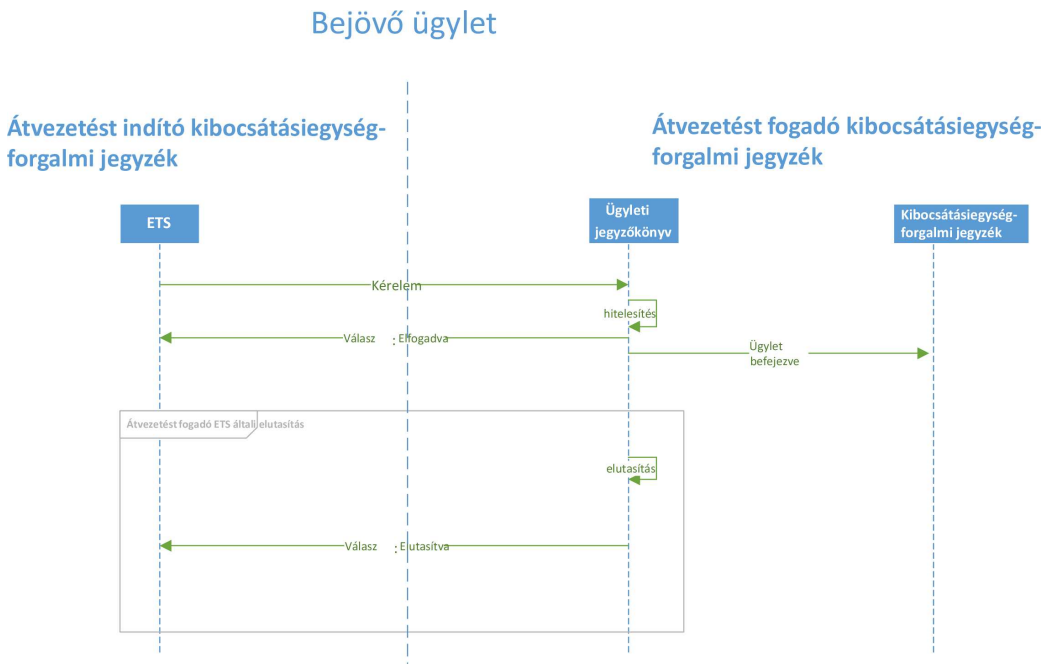
e) az átvezetést fogadó ETS ügyleti jegyzőkönyve nem érvényesíti az ügyletet;

f) az átvezetést fogadó ETS elküldi az elutasító választ az átvezetést indító ETS ügyleti jegyzőkönyvéhez;

g) az ügyleti jegyzőkönyv elküldi az elutasítást a kibocsátásiegység-forgalmi jegyzéknek.

Bejövő ügyletek

Ez az átvezetést fogadó ETS nézőpontját tükrözi. A konkrét folyamatot az alábbi folyamatábra jeleníti meg:



Az ábra a következőket mutatja:

1. amikor az átvezetést fogadó ETS ügyleti jegyzőkönyve érvényesíti a kérelmet, elküldi az elfogadó üzenetet az átvezetést indító ETS-nek, valamint „ügylet lezárva" üzenetet küld az átvezetést fogadó ETS kibocsátásiegység-forgalmi jegyzékének;

2. amikor egy bejövő kérelem elutasításra kerül az átvezetést fogadó ügyleti jegyzőkönyvben, az ügyleti kérelmet nem küldik el az átvezetést fogadó ETS kibocsátásiegység-forgalmi jegyzékének.

Protokoll

Az ügyleti üzenet ciklus csak két üzenetet foglal magában:

– átvezetést indító ETS → Átvezetést fogadó ETS ügyleti javaslat,

– átvezetést fogadó ETS → Átvezetést indító ETS ügyleti válasz: vagy Elfogadva vagy Elutasítva (az elutasítás indokával együtt):

  – Elfogadva: az ügyletet teljesítik,

  – Elutasítva: az ügyletet leállítják.

Az ügylet státusza

– Az átvezetést indító ETS ügyleti státusza „javasolt" lesz a kérelem elküldésekor.

– Az átvezetést fogadó ETS ügyleti státusza „javasolt" lesz a kérelem beérkezésekor és annak kezelése során.

– Az átvezetést fogadó ETS ügyleti státusza „teljesített"/„leállított" lesz, amikor a javaslat feldolgozásra kerül. Ezt követően az átvezetést fogadó ETS elküldi a megfelelő elfogadó/elutasító üzenetet.

– Az átvezetést indító ETS ügyleti státusza „teljesített"/„leállított" lesz, amikor az elfogadás/elutasítás beérkezik és feldolgozásra kerül.

– Az átvezetést indító ETS-ben az ügyleti státusz javasolt marad, amennyiben nem érkezik válasz.

– Az átvezetést fogadó ETS ügyleti státusza „leállított" lesz, ha bármely javasolt ügylet több mint 30 percen át „javasolt" státuszú marad.

Az ügyletekkel kapcsolatos események kezelése során be kell tartani a közös üzemeltetési eljárásokban foglalt eseménykezelési folyamatban meghatározott üzemeltetési eljárásokat.

3.2. *Adatátvitel biztonsága*

Az adatok továbbításuk során négy biztonsági szinten mennek át:

1. hálózati hozzáférés-vezérlés: tűzfal és hálózati összekapcsolási réteg;

2. titkosítás az átvitel szintjén: VPN vagy azzal egyenértékű biztonságos adatátviteli hálózat;

3. titkosítás a munkamenet szintjén: biztonságos üzenettovábbítási protokoll;

4. titkosítás az alkalmazás szintjén: XML-tartalom titkosítása és aláírása.

3.2.1. Tűzfal és hálózati összekapcsolás

A kapcsolat hardver alapú tűzfallal védett hálózaton keresztül jön létre. A tűzfal konfigurálása olyan szabályok alapján történik, hogy csak „regisztrált" kliensek kapcsolódhatnak a VPN-szerverhez.

3.2.2. Virtuális magánhálózat (VPN)

A Felek közötti kommunikáció minden esetben biztonságos adatátviteli technológiával védett. Virtuális magánhálózat (VPN) esetén az infrastruktúrának hardveren vagy virtuális készülékeken kell alapulnia. A VPN-technológiák lehetőséget nyújtanak a hálózaton – pl. az interneten – egyik ponttól a másikig történő, „alagúton" keresztüli áthaladásra, a kommunikációk mindenkori védelme mellett. A VPN alagút létrehozását megelőzően elektronikus tanúsítvány kiállítására kerül sor egy leendő kliens végpont részére, amely lehetővé teszi a kliens számára, hogy igazolja a személyazonosságát az összekapcsolás igénylése során. Mindegyik Fél felel azért, hogy saját VPN végpontján telepítse a tanúsítványt. Az elektronikus tanúsítványok használatával mindkét oldal VPN szervere hozzáférést kap egy központi hatósághoz a hitelesítő adatok egyeztetése érdekében. Az alagút-létrehozási folyamat során titkosítás kerül meghatározásra, biztosítva az alagúton keresztül zajló kommunikációk védelmét.

A kliens VPN végpontokat úgy kell konfigurálni, hogy biztosítva legyen a VPN alagút folyamatos fenntartása a Felek közötti megbízható, kétirányú, valós idejű kommunikáció mindenkori lehetővé tétele érdekében.

Bármely más, egyenértékű megoldásnak összehangban kell állnia a fent leírt elvekkel.

3.2.3. IPSec megvalósítása

VPN-megoldás alkalmazása esetén az IPSec protokollnak a helyek közötti VPN-infrastruktúra létrehozásához történő használata biztosítja a helyek közötti hitelesítést, az adatok sértetlenségét, valamint az adatok titkosítását. Az IPSec VPN konfigurációk biztosítják a VPN kapcsolat két végpontja közötti megfelelő hitelesítést. A Felek azonosítják és hitelesítik a távoli klienst az IPSec kapcsolaton keresztül, a másik oldal által elismert tanúsító hatóság által kiadott elektronikus tanúsítványok használatával.

Az IPSec továbbá biztosítja az adatok sértetlenségét a VPN alagúton keresztül zajló kommunikációk során. Az adatcsomagokat a VPN által létrehozott hitelesítési információk felhasználásával kivonatolják (hashed) és aláírják. Az adatok bizalmas jellegét hasonlóképpen, IPSec titkosítás lehetővé tételével biztosítják.

3.2.4. Biztonságos üzenettovábbítási protokoll

Az ideiglenes megoldás több titkosítási rétegre támaszkodik a Felek közötti biztonságos adatcsere érdekében. Mindkét rendszer és azok különböző környezetei a hálózat szintjén vannak összekapcsolva VPN alagutakon vagy azokkal egyenértékű biztonságos adatátviteli hálózatokon keresztül. Az alkalmazás szintjén a fájlok átvitelére biztonságos üzenettovábbítási protokoll alkalmazásával kerül sor munkamenet szinten.

3.2.5. XML titkosítás és aláírás

Az XML fájlokon belül az aláírás és a titkosítás két szinten történik. Minden ügyleti kérelem, ügyleti válasz és egyeztető üzenet egyenként kerül aláírásra, elektronikus úton.

A második lépésben az „üzenet” elem minden aleleme egyenként titkosításra kerül.

Ezen túlmenően a harmadik lépésben sor kerül a gyökérelem elektronikus úton történő aláírására, a teljes üzenet sértetlenségének és letagadhatatlanságának biztosítása érdekében. Ez az XML-be beágyazott adatok magas szintű védelmét eredményezi. A műszaki végrehajtásra a World Wide Web Konzorcium előírásaival összhangban kerül sor.

Az üzenet visszafejtéséhez ezt a folyamatot kell követni, fordított sorrendben.

3.2.6. Rejtjelezési kulcsok

A titkosítás és az aláírás nyilvános kulcsú kriptográfia alkalmazásával történik.

Az IPSec konkrét esetében mindkét Fél által megbízhatónak tartott tanúsító hatóság által kiállított elektronikus tanúsítványokat kell használni. Ez a tanúsító hatóság ellenőrzi a tanúsítvány birtokosának identitását, és olyan tanúsítványokat ad ki, amelyekkel a szervezetek egyértelműen azonosíthatók, és amelyek felhasználhatók a Felek közötti biztonságos adatkommunikációs csatornák létrehozásához.

A kommunikációs csatornák és az adatfájlok aláírására és rejtjelezésére rejtjelezési kulcsok alkalmazásával kerül sor. A nyilvános tanúsítványokat a Felek elektronikus úton cserélik ki egymással, biztonságos csatornákat használva, és azokat független csatornákon keresztül hitelesítik. Ez az eljárás a közös üzemeltetési eljárásokban foglalt információbiztonsági irányítási folyamat szerves részét képezi.

3.3. *A kapcsolat keretében végzett funkciók listája*

A kapcsolat meghatározza az átviteli rendszert a megállapodásból eredő üzleti folyamatokat végrehajtó funkciók vonatkozásában. A kapcsolat magában foglalja továbbá az egyeztetési folyamatra és a próbaüzenetekre vonatkozó előírást, ami lehetővé teszi a szívdobbanás-felügyelet megvalósítását.

3.3.1. Üzleti ügyletek

Üzleti szempontból a kapcsolat négy (4) típusú ügyleti kérelmet vesz figyelembe:

– Külső átvezetés:

  – az ETS-ek összekapcsolásának hatálybalépését követően az uniós és a svájci kibocsátási egységek helyettesíthetők, ezáltal pedig teljes mértékben átruházhatók a Felek között,

– a kapcsolaton keresztül végzett átvezetés egy átvezetést indító számlát érint az egyik ETS-ben és egy átvezetést fogadó számlát a másik ETS-ben,

– az átvezetés a négy (4) típusú kibocsátási egység bármekkora mennyiségét magában foglalhatja:

  – svájci általános célú kibocsátási egységek (CHU),

  – svájci légi közlekedési kibocsátási egységek (CHUA),

  – EU általános célú kibocsátási egységek (EUA),

  – EU légi közlekedési kibocsátási egységek (EUAA).

– Nemzetközi kiosztás:

  Azok a légijármű-üzembentartók, amelyek az egyik ETS igazgatása alá tartoznak, amely kötelezettségekkel bír a másik ETS felé, és amelyek jogosultak arra, hogy ettől a második ETS-től kibocsátási egységeket vegyenek át térítésmentesen, ingyenes légi közlekedési kibocsátási egységeket kapnak a második ETS-től a nemzetközi kiosztási ügylet útján.

– A nemzetközi kiosztás visszavonása:

  Erre az ügyletre akkor kerül sor, ha a légijármű-üzembentartó számlájára a másik ETS által kiosztott ingyenes kibocsátási egységeket teljes mértékben vissza kell vonni.

– Indokolatlanul kiosztott kibocsátásiegység-mennyiség visszaadása:

  Hasonló a visszavonáshoz, de ebben az esetben a kiosztást nem kell teljes mértékben visszavonni, csak a túlzott mennyiségben kiosztott kibocsátási egységeket kell visszaadni a kiosztó ETS-nek.

3.3.2. Egyeztetési protokoll

Az egyeztetésekre csak az üzenetek befogadására, hitelesítésére és feldolgozására rendelkezésére álló időkereten belül kerülhet sor.

Az egyeztetések az összekapcsolás biztonságára és a következetességére irányuló intézkedések szerves részét képezik. Bármely ütemterv elkészítése előtt a Felek megállapodnak az egyeztetés pontos időzítése tekintetében. Napi szinten ütemezett egyeztetésre is sor kerülhet, amennyiben ezt mindkét Fél elfogadja. Minimumkövetelményként legalább egy ütemezett egyeztetést kell végrehajtani minden befogadást követően.

Ugyanakkor bármelyik Fél bármikor kezdeményezhet manuális egyeztetéseket.

Az ütemezett egyeztetés időzítésében és gyakoriságában bekövetkező változások kezelése során be kell tartani a közös üzemeltetési eljárásokban foglalt kérésteljesítési folyamatban meghatározott üzemeltetési eljárásokat.

3.3.3. Próbaüzenet

A végpontok közötti kommunikáció tesztelése céljából próbaüzenetet kell küldeni. Az üzenet olyan adatokat tartalmaz, amelyek azt próbaüzenetként azonosítják, és az üzenet átvételét követően a másik végpont választ küld.

3.4. *Webszolgáltatásokra vonatkozó előírások*

Az ideiglenes megoldás során nem kerül sor webszolgáltatások igénybevételére. Meg kell azonban jegyezni, hogy az XML üzenetek alakja és formátuma nagyrészt változatlan marad. A kibocsátásiegység-forgalmi jegyzékek közötti állandó kapcsolat jövőbeni bevezetésével azonban a webszolgáltatásoknak lehetővé kell tenniük XML üzenetek valós idejű kicserélését.

3.5. *Webszolgáltatások specifikus meghatározása*

Ez a szakasz nem alkalmazandó az ideiglenes megoldás tekintetében. A fenti szakaszban foglaltak szerint a webszolgáltatások alkalmazására csak a kibocsátásiegység-forgalmi jegyzékek közötti állandó jövőbeni kapcsolat vonatkozásában kerül majd sor.

3.6. *Adatnaplózási követelmények*

Tekintettel arra, hogy mindkét Félnek szüksége van arra, hogy folyamatosan pontos és következetes információk álljanak rendelkezésükre, valamint az egyeztetési folyamat során a következetlenségek kiküszöböléséhez használható eszköz biztosítása érdekében a Feleknek négy (4) típusú adatrögzítést kell fenntartaniuk:

– Ügyleti jegyzőkönyvek,

– Egyeztetési jegyzőkönyvek,

– Üzenet archívum,

– Belső ellenőrzési jegyzőkönyvek.

Az ezekben a jegyzőkönyvekben rögzített adatokat legalább három (3) hónapig meg kell őrizni hibaelhárítási célokból, az adatok további megőrzése pedig az alkalmazandó jogtól függ mindkét végponton, ellenőrzés céljából. A három (3) hónapnál régebbi jegyzőkönyvfájlok egy független információtechnológiai rendszerben, biztonságos helyen archiválhatók úgy, hogy azok észszerű időn belül visszakereshetők és hozzáférhetők legyenek.

Ügyleti jegyzőkönyvek

Az EUTL és az SSTL alrendszer is tartalmaz ügyleti jegyzőkönyv megvalósításokat.

Pontosabban az ügyleti jegyzőkönyvek nyilvántartásként szolgálnak a másik ETS-nek küldött minden egyes javasolt ügyletről. Minden bejegyzés tartalmazza az ügyleti tartalom összes területét, valamint az ügylet későbbi kimenetelét (a fogadó ETS válasza). Az ügyleti jegyzőkönyvek nyilvántartást vezetnek továbbá a bejövő ügyletekről, valamint a származási ETS-nek küldött válaszról.

Egyeztetési jegyzőkönyvek

Az egyeztetési jegyzőkönyvben rögzítésre kerülnek a Felek egyeztetéssel kapcsolatos üzenetváltásai, beleértve az egyeztetési azonosítót, az időbélyegzőt és az egyeztetés eredményét is: Egyeztetési státusz: „Megfelel” vagy „Eltérések”. Az ideiglenes megoldásban az egyeztetési üzenetek az üzenetváltások szerves részét képezik.

Mindkét Fél köteles az egyeztetési jegyzőkönyvben rögzíteni minden kérelmet és az arra adott választ. Habár nem kerül sor az egyeztetési jegyzőkönyvben szereplő adatok közvetlen megosztására magának az egyeztetésnek a részeként, a következetlenségek kiküszöbölése érdekében szükség lehet az ilyen adatokhoz való hozzáférésre.

Üzenet archiválása

Mindkét Fél köteles archiválni a kicserélt – elküldött és beérkezett – adatok (az XML fájlok) egy példányát, valamint rögzíteni azt, hogy azok vagy az XML üzenetek megfelelő formátumúak voltak-e vagy sem.

Az archiválás elsősorban ellenőrzés céljából történik, hogy bizonyítékok álljanak rendelkezésre arra vonatkozóan, hogy mit küldtek el a másik Félnek, illetve mi érkezett a másik Féltől. Ebben az értelemben a fájlokkal együtt a kapcsolódó tanúsítványokat is archiválni kell.

Ezek a fájlok is további információkkal szolgálhatnak a hibaelhárításhoz.

Belső ellenőrzési jegyzőkönyv

Ezek a jegyzőkönyveket mindkét Fél önállóan határozza meg és használja.

3.7. *Üzemeltetési követelmények*

A két rendszer közötti adatcsere nem teljesen autonóm jellegű az ideiglenes megoldás során, ami azt jelenti, hogy szükség van üzemeltetőkre és eljárásokra a kapcsolat működőképessé tételéhez.

4. Elérhetőségre vonatkozó rendelkezések

4.1. *A kommunikáció elérhetőségének tervezése*

Az ideiglenes megoldás architektúráját alapvetően olyan IKT-infrastruktúra és szoftver képezi, amely lehetővé teszi a svájci ETS és az EU ETS közötti kommunikációt. Az ilyen adatáramlás magas szintű elérhetőségének, sértetlenségének és titkosságának a biztosítása ezért olyan lényeges szempont, amelyet figyelembe kell venni az ideiglenes megoldás és a kibocsátásiegység-forgalmi jegyzékek közötti állandó kapcsolat tervezése során. Tekintettel arra, hogy ez egy olyan projekt, amelyben az IKT-infrastruktúra, az egyedi szoftver és a folyamatok alapvető szerepet játszanak, mindhárom elemet figyelembe kell venni egy ellenállóképes rendszer kialakítása érdekében.

IKT-infrastruktúra ellenálló képessége

E dokumentum általános rendelkezéseket taglaló része tartalmazza az architektúra építőelemeinek leírását. Az IKT-infrastruktúra tekintetében az ideiglenes összekapcsolással létrejön egy ellenálló VPN hálózat (vagy azzal egyenértékű hálózat), amely biztonságos kommunikációs csatornákat hoz létre, amelyeken keresztül biztonságos üzenetváltásokra kerülhet sor. Az infrastruktúra többi eleme úgy van konfigurálva, hogy biztosítva legyen a magas szintű elérhetőség és/vagy tartalékmechanizmusok rendelkezésre állása.

Egyedi szoftver ellenálló képessége

Az egyedileg kifejlesztett szoftvermodulok növelik az ellenálló képességet azzal, hogy adott ideig újra megkísérlik a kommunikációt a másik Féllel, ha bármilyen oknál fogva az nem elérhető.

Szolgáltatás ellenálló képessége

Az ideiglenes megoldásban a Felek közötti adatcserékre előre meghatározott időrésekben kerül sor az év során. Az előre ütemezett adatcserék során előírt bizonyos lépéseknél szükség van a rendszerüzemeltetők és/vagy a jegyzékkezelők általi manuális beavatkozásra. Tekintettel erre, valamint a cserék elérhetőségének és eredményességének fokozása érdekében:

– az üzemeltetési eljárások jelentős időablakokat biztosítanak az egyes lépések végrehajtásához,

– az ideiglenes megoldáshoz tartozó szoftvermodulok aszinkron kommunikációt valósítanak meg,

– az automatikus egyeztetési folyamat kimutatja, hogy voltak-e problémák a másik oldalon az adatfájlok beolvasása során,

– az ellenőrzési folyamatokat (IKT-infrastruktúra és egyedi szoftvermodulok) figyelembe veszik az eseménykezelési eljárásokban, és azok elindítják ezeket az eljárásokat (a közös üzemeltetési eljárásokat tartalmazó dokumentumban meghatározottak szerint). Azok az eljárások, amelyek az eseményeket követően az üzemszerű működés helyreállításához szükséges idő lerövidítésére irányulnak, alapvető fontosságúak a magas elérhetőségi arányok biztosításához.

4.2. *Kezdeményezés, kommunikáció, újbóli aktiválás és vizsgálati terv*

Az ideiglenes megoldás architektúrájában foglalt összes különböző elemet egy sor egyéni és csoportos vizsgálatnak kell alávetni annak megerősítése érdekében, hogy a platform készen áll az IKT-infrastruktúra és az információs rendszer szintjén. Ezek a működési vizsgálatok kötelező előfeltételek tekintendők minden alkalommal, amikor a platform az ideiglenes megoldás állapotát átállítja felfüggesztettről működőképesre.

A kapcsolat működőképes állapotának aktiválásához ezt követően szükség van az előzetesen meghatározott vizsgálati terv sikeres kivitelezésére. Ez megerősíti, hogy mindegyik kibocsátásiegység-forgalmi jegyzék elvégzett először egy sor belső vizsgálatot, majd elvégezte a végpontok közötti hálózati összekapcsoltság érvényesítését, a Felek közötti gyártási ügyletek benyújtásának megkezdése előtt.

A vizsgálati tervnek tartalmaznia kell az átfogó vizsgálati stratégiát és a vizsgálati infrastruktúrára vonatkozó részleteket. Minden vizsgálati blokk minden egyes eleme tekintetében a tervnek különösen a következőket kell tartalmaznia:

– Vizsgálati kritériumok és eszközök,

– A vizsgálatok elvégzése érdekében kiosztott szerepek,

– Várt eredmények (pozitív és negatív),

– Vizsgálati ütemterv,

– A vizsgálati eredményekre vonatkozó követelmények rögzítése,

– Hibaelhárítási dokumentumok,

– Felterjesztésre vonatkozó rendelkezések.

A működőképes állapot aktiválására irányuló vizsgálatok folyamata négy (4) elvi blokkra vagy szakaszra osztható:

4.2.1. Belső IKT-infrastruktúra vizsgálatok

Ezeket a vizsgálatokat a Felek mindkét oldalon egyedileg végzik el és/vagy ellenőrzik.

Az IKT-infrastruktúra minden elemét mindkét oldalon egyedileg kell tesztelni. Ez kiterjed az infrastruktúra minden egyes alkotóelemére. Ezek a vizsgálatok elvégezhetők automatikusan vagy manuálisan, de igazolniuk kell, hogy az infrastruktúra minden eleme működőképes.

4.2.2. Kommunikációs vizsgálatok

Ezeket a vizsgálatokat egyedileg indíthatja el bármelyik Fél, és lefolytatásukhoz a másik oldal közreműködése szükséges.

Amint az egyes elemek működőképessé válnak, ellenőrizni kell a két kibocsátásiegység-forgalmi jegyzék közötti kommunikációs csatornákat. Ennek során mindkét Fél ellenőrzi, hogy van-e működőképes internet-hozzáférés, létrehozták-e a VPN-alagutakat (vagy azokkal egyenértékű biztonságos átviteli hálózatot), és van-e helyek közötti IP-kapcsolat. Ezt követően a másik oldalon meg kell erősíteni a helyi és távoli infrastruktúraelemek és az IP-kapcsolat elérhetőségét.

4.2.3. Az egész rendszerre kiterjedő (végpontok közötti) vizsgálatok

Ezeket a vizsgálatokat mindkét oldalon el kell végezni, és az eredményeket közölni kell a másik Féllel.

A kommunikációs csatornák, valamint a két kibocsátásiegység-forgalmi jegyzék minden egyes alkotóelemének vizsgálatát követően mindkét oldal szimulált ügyleteket és egyeztetést dolgoz ki, amelyek bemutatják a kapcsolat keretében végrehajtandó összes funkciót.

4.2.4. Biztonsági tesztek

Ezeket a teszteket mindkét Fél elvégzi és/vagy kezdeményezi mindkét oldalon, az 5.4. („Biztonsági tesztelésre vonatkozó útmutató") és az 5.5. („Kockázatértékelésre vonatkozó rendelkezések") szakaszban leírtak szerint.

Az ideiglenes kapcsolat csak azt követően tekinthető működőképes állapotúnak, hogy mind a négy szakasz/blokk kiszámítható eredményekkel lezárult.

Vizsgálati erőforrások

Mindkét Fél meghatározott vizsgálati erőforrásokra (meghatározott IKT-infrastruktúrára, szoftverre és hardverre) támaszkodik, továbbá a platform manuális és folyamatos hitelesítésének támogatása érdekében vizsgálati funkciókat fejleszt ki saját rendszeréhez. Az egyénileg vagy együttműködés keretében végzett manuális vizsgálati eljárások bármikor, bármelyik jegyzékkezelő által végrehajthatók. A működőképes állapot aktiválása önmagában véve manuális folyamat.

Az előírások szerint a platform rendszeres időközönként automatikus ellenőrzéseket is végez. Ezen ellenőrzések célja a platform elérhetőségének javítása az infrastruktúrával vagy a szoftverrel kapcsolatos problémák korai felismerése révén. Ez a platform ellenőrzési terv két elemből áll:

– IKT-infrastruktúra ellenőrzése: Az infrastruktúrát mindkét oldalon ellenőrzik az IKT-infrastruktúra szolgáltatók. Az automatikus vizsgálatok kiterjednek a különböző infrastruktúraelemekre és a kommunikációs csatornák elérhetőségére.

– Alkalmazás ellenőrzése: Az ideiglenes összekapcsolási szoftvermodulok az alkalmazás szintjén megvalósítják a rendszerkommunikáció ellenőrzését (manuálisan és/vagy rendszeres időközönként), melynek során megvizsgálják az összekapcsolás végpontok közötti elérhetőségét a kapcsolaton keresztül végzett bizonyos ügyletek szimulálása révén.

4.3. *Elfogadási/Tesztelési környezetek*

Az uniós kibocsátásiegység-forgalmi jegyzék és a svájci kibocsátásiegység-forgalmi jegyzék architektúrája az alábbi három környezetet foglalja magában:

– gyártási (Production – PROD): ez a környezet tartalmazza a valós adatokat és folyamatokat, valamint a valós ügyleteket,

– elfogadási (Acceptance – ACC): ez a környezet nem valós vagy anonimizált, reprezentatív adatokat tartalmaz. Ez az a környezet, ahol mindkét Fél rendszerüzemeltetői érvényesítik az új kiadásokat,

– tesztelési (Test – TEST): ez a környezet nem valós vagy anonimizált, reprezentatív adatokat tartalmaz. Ez a környezet a jegyzékkezelőkre korlátozódik, és az integrációs tesztek Felek általi elvégzésére szolgál.

A VPN (vagy más egyenértékű hálózat) kivételével a három környezet teljes mértékben független egymástól, ami azt jelenti, hogy a hardver, a szoftver, az adatbázisok, a virtuális környezetek, az IP-címek, a portok egymástól függetlenül kerülnek kialakításra, és azok egymástól függetlenül működnek.

Ami a VPN elrendezését illeti, az két különböző környezetben kerül létrehozásra, vagyis egy a PROD, egy másik független pedig az ACC és a TEST környezetben.

5. **Titoktartásra és sértetlenségre vonatkozó rendelkezések**

A biztonsági mechanizmusok és eljárások kétszemélyes módszert (négy szem elve) írnak elő az uniós kibocsátásiegység-forgalmi jegyzék és a svájci kibocsátásiegység-forgalmi jegyzék közötti kapcsolat során végzett műveletek vonatkozásában. Szükség esetén mindig a kétszemélyes módszer alkalmazandó. Ugyanakkor előfordulhat, hogy az nem alkalmazható a jegyzékkezelők által végzett valamennyi lépés esetén.

A biztonsági előírásokat figyelembe kell venni és követni kell a biztonságirányítási tervben, ami a biztonság esetleges megsértését követően a biztonsági események kezeléséhez kapcsolódó folyamatokat is magában foglalja. E folyamatok operatív részének a leírását a közös üzemeltetési eljárások tartalmazzák.

5.1. *Biztonsági tesztelési infrastruktúra*

A Felek vállalják, hogy mindegyikük biztonsági tesztelési infrastruktúrát hoz létre (a fejlesztés és az üzemeltetés szakaszában a sebezhetőségek felismeréséhez használt közös szoftverek és hardverek alkalmazásával):

– a gyártási környezettől elkülönítve,

– ahol a biztonság elemzését a rendszer fejlesztésétől és üzemeltetésétől független csoport végzi.

A Felek vállalják statikus és dinamikus elemzések végzését egyaránt.

Dinamikus elemzés (pl. behatolási tesztelés) esetén a Felek vállalják, hogy az értékeléseket általában a tesztelési és az elfogadási környezetekre korlátozzák (az „Elfogadási/Tesztelési környezetek" című 4.3. szakaszban foglaltak szerint). E szabálytól kizárólag mindkét Fél jóváhagyása esetén lehet eltérni.

A gyártási környezetben való telepítést megelőzően a kapcsolat minden szoftvermodulját („A kommunikációs kapcsolat architektúrája" című 3.1. szakaszban foglaltak szerint) tesztelni kell.

A tesztelési infrastruktúrát a hálózat és az infrastruktúra szintjén egyaránt el kell különíteni a gyártási infrastruktúrától. A biztonsági előírásoknak való megfelelés ellenőrzéséhez szükséges biztonsági teszteket a tesztelési infrastruktúrában kell elvégezni.

5.2. *A kapcsolat felfüggesztésére és újbóli aktiválására vonatkozó rendelkezések*

Amennyiben felmerül annak a gyanúja, hogy a svájci kibocsátásiegység-forgalmi jegyzék, az SSTL, az uniós kibocsátásiegység-forgalmi jegyzék vagy az EUTL biztonsága veszélybe került, a Felek haladéktalanul tájékoztatják egymást, és felfüggesztik az SSTL és az EUTL közötti kapcsolatot.

Az információk megosztására, valamint a felfüggesztésről és az újbóli aktiválásról szóló határozat meghozatalára vonatkozó eljárások a közös üzemeltetési eljárásokban foglalt kérésteljesítési folyamat részét képezik.

Felfüggesztések

A kibocsátásiegység-forgalmi jegyzékek közötti kapcsolatnak a megállapodás II. melléklete szerinti felfüggesztésére az alábbiak miatt kerülhet sor:

– adminisztratív okok (például karbantartás), ami tervezett,

– biztonsági okok (vagy az informatikai infrastruktúra meghibásodásai), ami nem tervezett.

Veszélyhelyzetben az egyik Fél tájékoztatja a másik Felet és egyoldalúan felfüggeszti a kibocsátásiegység-forgalmi jegyzékek közötti kapcsolatot.

Amennyiben határozat születik a kibocsátásiegység-forgalmi jegyzékek közötti kapcsolat felfüggesztéséről, a Felek ennek megfelelően biztosítják a kapcsolat hálózati szinten történő megszakítását (a bejövő és kimenő kapcsolatok részben vagy teljes egészében történő blokkolásával).

A kibocsátásiegység-forgalmi jegyzékek közötti kapcsolat – akár tervezett, akár nem tervezett – felfüggesztéséről szóló határozat meghozatalára a közös üzemeltetési eljárásokban foglalt változáskezelési eljárás vagy biztonsági események kezelésére vonatkozó eljárás szerint kerül sor.

A kommunikáció újbóli aktiválása

A kibocsátásiegység-forgalmi jegyzékek közötti kapcsolat újbóli aktiválására vonatkozó határozat meghozatalára a közös üzemeltetési eljárásokban foglaltak szerint kerül sor, és semmi esetre sem az 5.4. („Biztonsági tesztelésre vonatkozó útmutató") és a 4.2. („Kezdeményezés, kommunikáció, újbóli aktiválás és vizsgálati terv") című szakaszban leírt biztonsági tesztelési eljárások sikeres befejezése előtt.

5.3. *A biztonság megsértésére vonatkozó rendelkezések*

A biztonság megsértése az érzékeny információk bizalmasságát és sértetlenségét és/vagy az ilyen információkat kezelő rendszer elérhetőségét érintő biztonsági eseménynek minősül.

Az érzékeny információk az Érzékeny információk jegyzékében kerülnek meghatározásra, és azok a rendszerben vagy a rendszer bármely kapcsolódó részében kezelhetők.

A biztonság megsértéséhez közvetlenül kapcsolódó információk érzékenynek tekintendők, „ETS CRITICAL” (ETS kritikus jelentőségű információ) megjelölést kapnak, és eltérő rendelkezések hiányában azokat a kezelési utasításokkal összhangban kell kezelni.

A biztonság megsértését minden esetben a közös üzemeltetési eljárások „Biztonsági események kezelése” című fejezetében foglaltak szerint kell kezelni.

5.4. *Biztonsági tesztelésre vonatkozó útmutató*

5.4.1. Szoftver

A biztonsági tesztelést, adott esetben ideértve a behatolási tesztelést, legalább a szoftver összes főbb új kiadásán el kell végezni az LTS-ekben foglalt biztonsági előírások szerint, az összekapcsolás biztonsági szintjének és a kapcsolódó kockázatoknak az értékelése érdekében.

Amennyiben az elmúlt 12 hónapban nem készült jelentős kiadás, a biztonsági tesztelést a meglévő rendszeren kell elvégezni, figyelembe véve a számítógépes fenyegetések alakulását az elmúlt 12 hónapban.

A kibocsátásiegység-forgalmi jegyzékek közötti kapcsolat biztonsági tesztelését az elfogadási környezetben kell elvégezni, valamint – szükség esetén – a gyártási környezetben, a Felek közötti koordináció és kölcsönös megállapodás keretében.

A webes alkalmazások tesztelése során be kell tartani a nemzetközi nyílt szabványokat, köztük az Open Web Application Security Project (OWASP) keretében kidolgozott előírásokat.

5.4.2. Infrastruktúra

A gyártási rendszert támogató infrastruktúrát rendszeresen (legalább havonta egyszer) át kell vizsgálni a sebezhetőségek felismerése érdekében, és az észlelt sebezhetőségeket ki kell javítani. A tesztelést az 5.4.1. szakaszban ismertetett elv alapján kell elvégezni naprakész sebezhetőségi adatbázis segítségével.

5.5. *Kockázatértékelésre vonatkozó rendelkezések*

Amennyiben szükség van behatolási tesztelésre, azt a biztonsági tesztelés keretében kell elvégezni.

A biztonsági tesztelés elvégzésére a Felek szerződést köthetnek egy erre szakosodott vállalattal, feltéve, hogy az adott vállalat:

– rendelkezik az ilyen biztonsági teszteléshez szükséges készségekkel és tapasztalattal,

– nem közvetlenül a fejlesztőnek és/vagy a fejlesztő alvállalkozójának jelentő vállalat, továbbá nem vesz részt a kapcsolat szoftverének fejlesztésében, és nem a fejlesztő alvállalkozója,

– titoktartási megállapodást írt alá, amelyben vállalta, hogy az eredményeket bizalmasan, a kezelési utasításoknak megfelelően ETS kritikus jelentőségű információként kezeli.